DATE(S) ISSUED:
7/13/2010

SUBJECT:
Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (MS10-044)

OVERVIEW:
Vulnerabilities have been discovered in Microsoft Office Access ActiveX control that could allow an attacker to take complete control of a vulnerable system. Microsoft Office Access is a database management system. ActiveX controls are small programs or animations that are downloaded or embedded in web pages which will typically enhance functionality and user experience. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email, which are specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

> Microsoft Access 2003
> Microsoft Access 2007

RISK:

Government:
> Large and medium government entities: **High**
> Small government entities: **High**

Businesses:
> Large and medium business entities: **High**
> Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been discovered in Microsoft Office Access ActiveX control that could allow an attacker to take complete control of a vulnerable system.

The first vulnerability is due to Internet Explorer incorrectly allocating memory. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities.

The second vulnerability occurs due to memory corruption in ActiveX controls in the ACCWIZ library. A remote code execution vulnerability exists in the way that the FieldList ActiveX control is instantiated by Microsoft Office and Internet Explorer. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email, which contains specifically crafted ActiveX controls with persisted storage data.

Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Configure email-clients to preview messages in plain-text format, rather than RTF or HTML format.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-044.mspx

VUPEN:
http://www.vupen.com/english/advisories/2010/1799

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0814
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1881